P/11077US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION PAPERS OF

LEE CODEL LAWSON TARBOTTON, EDWARD MOORE AND DANIEL JOSEPH WOLFF

FOR

EVENT REPORTING BETWEEN A REPORTING COMPUTER AND A RECEIVING COMPUTER

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the field of data processing systems. More particularly, this invention relates to event reporting between a reporting computer and a receiving computer, such as, for example, reporting the detection of a computer virus to an anti-virus software provider.

Description of the Prior Art

It is known to provide anti-virus computer programs that act to detect computer viruses and, if required, disinfect/clean/quarantine/delete infected files. When a computer virus is detected, the known systems may generate a virus detection report that is displayed to a user to inform them of the detection event. The user may at this time be given the option of accessing a description of the nature and action of the detected computer virus with that description either being stored locally or remotely. The generation of such descriptive information is labour intensive and expensive. With many tens of thousands of known computer viruses it is difficult to determine accurately which are the common computer viruses upon which users are requesting information in order that the resources for providing such information may be concentrated on these requests.

A further problem in the anti-virus field is obtaining an accurate picture of which viruses are at any time prevalent in the user community as well as obtaining an accurate picture of what anti-virus program tools with their different versions and update states are being used to counter these virus threats.

SUMMARY OF THE INVENTION

Viewed from one aspect the present invention provides a computer program product comprising a computer program operable to control a reporting computer to report occurrence of an event to a receiving computer, said computer program comprising:

report generating logic operable to generate report data identifying said reporting computer and said event;

data retrieving logic operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

report sending logic operable to send said report data from said reporting computer to said receiving computer upon fetching of said requested data.

The invention recognises that a report identifying a particular event and a computer upon which that event occurs may be passed to a receiving computer in combination with a request for data made from the reporting computer to the receiving computer in the course of other operation. Thus, the report can be made without having to establish a dedicated reporting communication session and without requiring a user to take any actions dedicated to triggering such a report. Rather, in the normal process of requesting data that is needed for other purposes, the reporting data may be passed on to the receiving computer at the same time.

It will be appreciated that the events being detected and reported could take a wide variety of forms. As an example, system malfunctions could be the subject of report data that was reported back to a system provider effectively "piggy backing" on a request for other data from that system provider.

Whilst the technique of the invention could be used in a wide variety of situations, it is particularly useful when the events being reported are the detection of computer viruses. The need to collect such data is high.

The requested data could take a variety of forms, but particularly preferred forms are when the requested data is a description, such as a web page, of the event being reported or when the requested data is an update to a set of data used in detecting such events.

A particularly efficient way of passing the report data is to create an internet URL in which the report data is embedded, preferably in an encrypted form to resist tampering, with

the receiving computer using the URL to trigger return of appropriate requested data as well as retrieving the report data from the URL.

In another set of embodiments, the report data may be locally collected by the reporting computer and then sent together as a collated report to the receiving computer at a later time.

The internet provides a particularly convenient link between the reporting computer and the receiving computer that may be used to transfer the report data and the requested data.

The report data could include many different data fields. Particularly advantageous data fields to be included within the report data include a MAC address that can be used to uniquely identify the reporting computer (a MAC address is practically unique, but it is possible to have duplicates and some network cards allow modification of the MAC address), date and time information, information identifying a computer program, version and update status of the computer program used to detect the event, data indicating the type of response that may have occurred on the reporting computer when the event was detected and possibly a checksum for verifying the identity of a computer file that may have triggered the event.

A complementary aspect of the invention is provided by a computer program product comprising a computer program operable to control a receiving computer to receive a report of occurrence of an event from a reporting computer, said computer program comprising:

data request receiving logic operable to receive a request for requested data from said reporting computer;

data providing logic operable to provide said requested data to said reporting computer; and

report receiving logic operable to receive report data identifying said reporting computer and said event from said reporting computer upon providing of said requested data to said reporting computer.

The invention also provides a method for operating a reporting computer and a receiving computer in accordance with the above techniques as well as a reporting computer and a receiving computer operating in accordance with the above techniques.

Embodiments of the invention will now be described, by way of example only, but with reference to the accompanying drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 schematically illustrates a reporting computer and a receiving computer;

Figure 2 illustrates the use of a URL to access requested data and to pass report data;

Figures 3 and 4 are flow diagrams respectively illustrating the operation of a reporting computer and a receiving computer in accordance with a first embodiment;

Figures 5 and 6 are flow diagrams respectively illustrating the operation of a reporting computer and a receiving computer in accordance with a second embodiment;

Figure 7 is a table illustrating the relationship between viruses and the virus driver number for various virus definition libraries;

Figure 8 is a table illustrating various data describing characteristics of certain computer viruses; and

Figure 9 is a table illustrating a collection of report data relating to various virus detections; and

Figure 10 is a diagram schematically illustrating a general purpose computer that provides one example of a system that may be used to implement the techniques of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 illustrates a reporting computer 2 connected via an internet link 4 to a receiving computer 6. The reporting computer 2 is a user's PC running anti computer virus

software stored upon a hard disc drive 8. A network card 10 having a unique MAC address connects the reporting computer to the receiving computer 6. The anti-virus software is made up of an anti-virus computer program engine having a particular version number that operates using a set of virus definition data having a particular update status.

The receiving computer 6 is the web server of an anti-virus provider. This web server includes a virus information library 12 comprising a collection of web pages that may be viewed by users to give a description of the nature and action of various computer viruses. A virus detection report log 14 within the receiving computer logs detection reports received from users. These detection reports may then be used to generate information regarding the real life prevalence of particular viruses, requests for information and the real life program versions and update status of users. The receiving computer 6 also includes virus definition data updates 16 that may be downloaded by users either on-demand or as part of a regular scheduled update process.

When the reporting computer 2 detects a computer virus, either as a result of on-access scanning or on-demand scanning, a virus detection report is generated and displayed to the user. This virus detection report includes a hypertext link 18 upon which the user may click if they wish to view a description of the virus that has been detected. This description is retrieved from the virus information library 12. The URL used to access to relevant page within the virus information library 12 upon activation of the hypertext link 18 also carries information uniquely identifying the reporting computer and the virus detection event.

Figure 2 illustrates the URL described above in more detail. In particular, the URL 20 includes the name of a script 22 running on the receiving computer 6 that takes encrypted data 24 passed within the URL 20 and uses this to recover reporting computer and event identifying data 26.

The encrypted data 24 is generated by the reporting computer 2 using known encryption techniques. The receiving computer 6 has a complimentary decryption key that enables it to recover the report data 26 from the encrypted data 24. The report data 26

includes the MAC address of the network card 10 of the reporting computer 2, the date and time at which the virus was detected, an identifier of the virus detection program used, an identifier of the anti-virus engine within that program, an identifier of the virus definition data current within that program together with an identifier of the particular driver of that was triggered by the virus file (the driver identifier may be mapped to the identity of the virus).

The URL 20 is not displayed on the reporting computer 2 but instead is effectively hidden behind a hypertext link 18 that invites the user to click upon it in order to see a description of the virus. When the user clicks upon the hypertext link 18, the URL request 20 is passed to the receiving computer 6. The receiving computer 6 uses the update number of the virus definition data together with the driver triggered data to identify the particular web page describing the virus concerned within the virus information library 12 and returns this web page 28 to be displayed upon the reporting computer 2. The receiving computer 6, also uses the report data 26 passed to it to generate a virus detection report log record 30 within a database of such records. This record may include the MAC address, the date, the time, the product identifier, the engine identifier, the virus definition data identifier and the driver triggered identifier as well as other information, such as the nature of the corrective action taken by the reporting computer (such as cleaning, quarantining or ignoring) as well as a checksum value for the file within which the virus was detected in order to assist in eliminating multiple reports of detection of the virus within the same file.

The database of records obtained by the receiving computer 6 in this way may be used to provide real life information regarding the prevalence of particular viruses in the user community together with real life information regarding the set up of those users anti-virus systems. The frequency at which information describing a particular virus, such as the web page information 28, is requested may be used to prioritise the generation of such descriptive data to be added to the virus information library 12.

Figure 3 illustrates the operation of a reporting computer 2 in accordance with a first embodiment. At step 32 a virus is detected. At step 34 a URL unique to that computer and

the detected virus event is generated, the reporting data being encrypted within the URL. At step 36 the virus report is displayed to the user. If the user clicks upon the hypertext link for more information regarding the virus detected, then step 38 sends the URL to the receiving computer 6 and fetches the relevant virus description web page 28.

Figure 4 illustrates the operation of a receiving computer in accordance with the first embodiment. At step 40 a URL request (as generated at step 38) is received. At step 42 the report data 26 embedded within the URL 20 is decrypted. At step 44 the virus description web page 28 is returned to the reporting computer 2 based upon the driver identifier and virus definition data identifier information recovered from the encrypted data 24. At step 46 the new virus detection report data 30 is appended to the database of such data held within the receiving computer 6. The request for the virus information may also be logged in order to identify the data being frequently requested by users in order that resources can then be focused on generating this data.

Figure 5 illustrates the action of a reporting computer in accordance with a second embodiment. At step 48 a virus is detected on the reporting computer 2. At step 50 a virus detection report is generated locally within the reporting computer 2 and appended to a local log of such reports held within the reporting computer 2. At step 52, at the same time as an on-demand virus definition data update or a scheduled virus definition data update, the reporting computer 2 establishes a connection to retrieve update data from the receiving computer 6. When this connection has been made, step 54 then serves to send the local log of virus detection reports from the reporting computer 2 to the receiving computer 6. Step 56 downloads the virus definition update data 16 from the receiving computer 6.

The reporting computer 2 in the embodiment of Figure 5 may be a centralised reporting computer used by all of the client computers on a network to co-ordinate their reporting of virus detection events to the anti-virus software provider. The local log of virus detection events held by this computer may also prove useful to a system administrator in identifying exactly what viruses have been detected within their network, together with when and where these viruses were detected.

Figure 6 illustrates the action of the receiving computer 6 in accordance with the second embodiment. At step 58, a connection request is received from the reporting computer 2. This connection request is to download the latest virus definition data 16. At step 60, the receiving computer 6 receives the collated log data that has been generated since the last report from the reporting computer 6 and appends this to its central database of virus detection reports. Step 62 may analyse this virus detection report data to allocate a priority to supplying the updated virus definition data to that particular reporting computer. Accordingly, a reporting computer that sends data indicative of a serious and widespread virus outbreak at that user site may receive a high priority for update download from the anti-virus system provider. Step 64 appends the received virus detection report data to the central log. Step 66 sends the virus definition update data to the reporting computer 2 in accordance with the determined priority.

The virus detection reports should be resistant to tampering and faking. It is important that if virus detection data is to be collected, then this data should be accurate as possible. The encryption of the report data within the URL 20 is one mechanism for protecting this data. The collated report data passed as described in connection with Figures 6 and 7 may also be encrypted in a similar manner.

Another way in which the virus detection data may be distorted is if multiple reports of the same virus detection events are received and separately logged. For this reason, the MAC address, date, time, driver identifier and file checksum mentioned above may be used to uniquely identify a virus detection event and accordingly identify duplicates that are reported to the receiving computer 6, such that undesired duplicates may be removed.

Figure 7 illustrates a table illustrating how for four different versions of the virus definition (DAT) data 68, the virus driver 70 triggered on a particular virus detection event may be used to map back to the virus sample number and virus name concerned.

Having identified the virus sample with a look up in the table of Figure 7, the virus description together with other virus characterising information may be looked up in the virus information library 12 using the table as illustrated in Figure 8.

Figure 9 illustrates a plurality of virus detection event reports. This collection of reports may be part of the database of such reports that is collected within the receiving computer 6, or alternatively might be part of the local collection of such reports made by a reporting computer 2 prior to sending these reports to the receiving computer 6 in accordance with the embodiments of Figures 5 and 6. As will be seen from entries 72 and 74 in Figure 9, entry 74 is a duplicate of entry 72. This may be detected unambiguously by the receiving computer 6 and the entry 74 deleted such that it does not distort the information recovered from the report data.

Figure 10 illustrates a general purpose computer 200 of the type that may be used to perform the above described techniques. The general purpose computer 200 includes a central processing unit 202, a read only memory 204, a random access memory 206, a hard disk drive 208, a display driver 210 with attached display 211, a user input/output circuit 212 with attached keyboard 213 and mouse 215, a network card 214 connected to a network connection and a PC computer on a card 218 all connected to a common system bus 216. In operation, the central processing unit 202 executes a computer program that may be stored within the read only memory 204, the random access memory 206, the hard disk drive 208 or downloaded over the network card 214. Results of this processing may be displayed on the display 211 via the display driver 210. User inputs for triggering and controlling the processing are received via the user input/output circuit 212 from the keyboard 213 and mouse 215. The central processing unit 202 may use the random access 206 as its working memory. A computer program may be loaded into the computer 200 via a recording medium such as a floppy disk drive or compact disk. Alternatively, the computer program may be loaded in via the network card 214 from a remote storage drive. The PC on a card 218 may comprise its own essentially independent computer with its own working memory, CPU and other control circuitry that can co-operate with the other elements in Figure 4 via

the system bus 216. The system bus 216 is a comparatively high bandwidth connection allowing rapid and efficient communication.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.